Cybersecurity Law and Digital Payment Systems: Protecting Consumers in the FinTech Era — With Special Focus on Cambodia

Dr. Sat Dara

School of Law and Government, Norton University, Phnom Penh, Cambodia

Cybersecurity Law and Policy Review

Volume 1, Issue 1 | 2025 | https://clprj.com/journal/index

Abstract

The explosive growth of financial technology and digital payment systems across Southeast Asia has generated unprecedented economic inclusion for millions of previously unbanked consumers while simultaneously creating a vast and insufficiently governed attack surface for cybercriminals, fraudsters, and state-affiliated threat actors. Nowhere is this paradox more acutely illustrated than in Cambodia, where a decade of aggressive digital financial infrastructure development — anchored by the National Bank of Cambodia's KHQR standardised QR payment system and the Bakong blockchain-based retail payment platform — has elevated financial access among the rural poor while coinciding with Cambodia's emergence as a global epicentre of cyber-enabled financial crime, money laundering through digital payment channels, and the exploitation of regulatory arbitrage by criminal enterprises operating in the country's governance-weak border zones. This article examines the cybersecurity legal framework governing digital payment systems, with Cambodia as its central analytical lens. Drawing on comparative regulatory analysis across the European Union, the United States, Singapore, Thailand, and the ASEAN region, the article assesses the adequacy of existing consumer protection law, payment system regulation, cybersecurity standards, and anti-money laundering frameworks to address the threats that digital payment systems face in the FinTech era. It analyses Cambodia's specific regulatory architecture — the Law on Financial Management, the Payment Systems Law, the National Bank of Cambodia's regulatory framework, and the nascent data protection and cybercrime legal instruments — against the backdrop of the country's dual role as a FinTech innovator and a centre of cyber-enabled financial crime. The article identifies the structural legal deficiencies that prevent effective consumer protection in Cambodia's digital payment ecosystem and advances a normative programme for legal reform that is attentive to Cambodia's development context, its regional integration obligations under ASEAN, and the urgent imperative of disrupting the criminal exploitation of its digital financial infrastructure.

Keywords: *Cambodia; digital payments; FinTech; cybersecurity law; Bakong; KHQR; consumer protection; financial crime; AML/CFT; ASEAN; payment fraud; cryptocurrency; data protection; financial inclusion*

1. INTRODUCTION

In October 2020, the National Bank of Cambodia (NBC) launched Bakong — a blockchain-based, interoperable retail payment system that is widely regarded as one of the most innovative central bank digital currency infrastructure projects in the developing world. Built on a permissioned blockchain developed in collaboration with Japanese FinTech company Soramitsu, Bakong enables real-time interbank transfers, QR code payments, and cross-border remittances at near-zero cost for users, with the potential to dramatically reduce Cambodia's high dependence on the US dollar and to extend financial services to the approximately 30 percent of Cambodians who remained unbanked at the system's launch. By 2024, Bakong had registered over ten million users — in a country of approximately seventeen million people — processed transactions totalling tens of billions of US dollars annually, and attracted international attention as a model of central bank-led digital payment infrastructure development for emerging economies.

The Bakong story is, in many respects, genuinely remarkable — an illustration of the capacity of digital financial infrastructure to accelerate financial inclusion and economic development in ways that conventional bank branch expansion could not achieve at comparable speed or cost. Yet the same digital payment infrastructure that has extended financial access to Cambodian smallholders, garment workers, and micro-entrepreneurs has also provided a sophisticated laundering channel for the billions of dollars generated by the scam compound operations that have made Cambodia internationally notorious. The same QR payment standardisation that enables a rice farmer in Kampong Cham to pay her mobile phone bill without visiting a bank branch has been exploited by criminal networks to move fraud proceeds through layered payment chains that defeat conventional financial intelligence analysis. The same cross-border remittance functionality that enables Cambodian migrant workers in Thailand to send money home to their families has been appropriated by criminal enterprises to transfer value across borders with a speed and opacity that anti-money laundering systems were not designed to intercept.

This juxtaposition — of legitimate financial innovation and criminal exploitation occurring simultaneously through the same digital infrastructure, in the same jurisdiction, with the same regulatory framework nominally governing both — encapsulates the central challenge of cybersecurity law and consumer protection in the FinTech era. Digital payment systems create value by enabling rapid, low-friction, widely accessible financial transactions; but the properties that create this value — speed, accessibility, low friction, interoperability, and often relative anonymity — are precisely the properties that criminal actors exploit. The regulatory framework must protect consumers against the cybersecurity threats and frauds enabled by digital payment systems without destroying the properties that make those systems socially valuable. In Cambodia's specific context, this regulatory challenge is further complicated by institutional capacity constraints, governance integrity deficits, and the particular intensity of the criminal exploitation of the country's digital financial infrastructure.

This article proceeds as follows. Part Two examines the global landscape of digital payment system cybersecurity threats, with particular attention to the threat vectors most prevalent in the Southeast Asian context. Part Three provides a detailed analysis of Cambodia's digital payment ecosystem and regulatory framework. Part Four surveys the international and comparative regulatory approaches to digital payment security and consumer protection. Part Five examines the specific intersection of Cambodia's digital payment infrastructure with the country's cyber-enabled financial crime ecosystem. Part Six analyses the structural deficiencies of Cambodia's legal framework for digital payment consumer protection. Part Seven advances a normative reform agenda. Part Eight concludes.

2. CYBERSECURITY THREATS TO DIGITAL PAYMENT SYSTEMS IN THE FINTECH ERA

2.1 The Evolving Threat Landscape

Digital payment systems have become one of the primary targets of cybercriminal activity globally, with the combination of high transaction volumes, direct access to financial value, and the irreversibility of successful fraudulent transactions making them structurally attractive to attackers across the sophistication spectrum. The threat landscape facing digital payment systems encompasses technically sophisticated attacks on payment infrastructure — including the infamous 2016 Bangladesh Bank SWIFT heist in which attackers stole $81 million by compromising the central bank's SWIFT messaging interface — alongside mass consumer-facing fraud schemes that exploit the usability features of modern payment applications to deceive ordinary users into authorising fraudulent transfers.

The taxonomy of digital payment threats is broad and continues to evolve as attackers adapt to defensive measures and exploit new payment modalities. Account takeover fraud — in which attackers compromise consumer payment accounts through credential theft, SIM swapping, or social engineering — remains among the most prevalent and economically significant threat categories, with global losses estimated in the tens of billions of dollars annually. Authorised push payment (APP) fraud — in which consumers are deceived into authorising transfers to accounts controlled by fraudsters through impersonation scams, investment fraud (including the pig butchering schemes documented in Cambodia's criminal ecosystem), and purchase scams — has become the dominant fraud typology in markets with well-developed instant payment infrastructure, precisely because the immediacy and irreversibility of instant payments maximises the fraudster's advantage.

Payment infrastructure attacks targeting the processing systems, switching networks, and API interfaces through which digital payments are routed represent a category of threat with potentially systemic consequences — the compromise of a single payment switch or processing hub can simultaneously affect millions of transactions and thousands of merchants and consumers. The 2013 Spamhaus DDoS attacks that temporarily disrupted internet infrastructure globally, and more recent attacks on regional payment processors, illustrate the vulnerability of centrally routed payment infrastructure to denial-of-service and intrusion attacks. The growing interconnection of payment systems through open banking APIs — mandated by regulatory frameworks including the EU's Payment Services Directive 2 (PSD2) — while generating significant consumer benefit, has substantially expanded the attack surface available to adversaries who can exploit insecure or poorly authenticated API connections.

2.2 QR Code Payment Fraud

QR code payment systems — which have achieved dominant market positions across Southeast Asia, including in Cambodia's KHQR ecosystem — present specific security challenges that have generated a substantial and growing fraud problem across the region. The fundamental vulnerability of QR code payments lies in the substitution attack: a fraudster replaces a legitimate merchant's QR code with a fraudulent code linking to the fraudster's payment account, redirecting consumer payments away from the legitimate merchant. This attack requires no technical sophistication — only physical access to the point of sale for long enough to substitute the code — yet can victimise dozens or hundreds of consumers before detection. Documented QR code substitution attacks across Southeast Asia, including in Cambodia, Thailand, Singapore, and China, have inflicted significant losses on both consumers (who lose the value of misdirected payments) and merchants (who do not receive payment for goods and services provided).

More sophisticated QR code payment fraud involves the creation of fake merchant applications or payment portals that generate QR codes linking to fraudster-controlled accounts, the impersonation of legitimate payment platforms through phishing websites and fraudulent mobile applications, and the exploitation of dynamic QR code generation systems where the code itself can be manipulated to redirect payments. The social engineering dimension of QR code payment fraud — in which fraudsters send QR codes purportedly enabling loan receipts, government benefit payments, or prize winnings that, when scanned, initiate payments from the victim's account rather than to it — represents a particularly insidious variant that exploits consumer unfamiliarity with the distinction between QR codes that receive and those that send payment.

2.3 Cryptocurrency and Stablecoin Risks in Payment Ecosystems

The integration of cryptocurrency and stablecoin functionality into digital payment ecosystems — a feature of Cambodia's Bakong system, which supports USDT (Tether) transactions alongside Cambodian riel transfers — introduces a set of cybersecurity and consumer protection challenges that are distinct from those arising in conventional fiat payment systems. Cryptocurrency transactions are generally irreversible once confirmed on the blockchain, providing fraudsters with a degree of finality that exceeds even that of instant fiat payment systems; they may be pseudonymous or, in the case of privacy coins, genuinely anonymous; and they operate through technical infrastructure (private keys, wallet addresses, seed phrases) whose loss or compromise irreversibly destroys access to the associated funds with no recourse to a central authority.

The use of USDT and other stablecoins as payment instruments in Cambodia is particularly significant from a legal and regulatory perspective. Tether (USDT), the most widely used stablecoin globally, is not issued by a regulated financial institution in any major jurisdiction and is not subject to the consumer protection, deposit insurance, or prudential regulatory frameworks applicable to conventional payment instruments. Its widespread use in Cambodia's digital payment ecosystem — both for legitimate cross-border remittances and, pervasively, for the settlement of criminal proceeds from scam compound operations — creates a regulatory gap that Cambodia's central bank and financial supervisory authorities lack the tools to address effectively without broader international cooperation.

3. CAMBODIA'S DIGITAL PAYMENT ECOSYSTEM: INNOVATION, INCLUSION, AND VULNERABILITY

3.1 The Architecture of Cambodia's Digital Payment System

Cambodia's digital payment landscape is characterised by a degree of innovation and infrastructure development that significantly outpaces the country's broader economic and institutional development, a consequence of deliberate government and central bank policy prioritising digital financial infrastructure as a development accelerator. The National Bank of Cambodia's Bakong system, launched in 2020, occupies the apex of the payment infrastructure hierarchy as a central bank-operated, blockchain-based interbank settlement system that provides the real-time settlement rails upon which commercial payment services are built. Bakong's architecture is notable for its technology choices — the use of a permissioned blockchain for settlement, rather than the conventional centralised real-time gross settlement (RTGS) systems used by most central banks — and for the NBC's decision to extend direct access to the system not only to licensed banks but to licensed payment service providers and, through them, to the general public.

Complementing Bakong is the KHQR standard, a unified QR code payment specification developed by the NBC and promulgated as the mandatory standard for QR code payments in Cambodia. KHQR adoption has been driven by NBC regulatory requirements that all payment service providers implement KHQR-compatible interfaces, creating an interoperable QR payment ecosystem across the country's licensed payment providers. The KHQR standard incorporates technical security specifications derived from the EMVCo QR code standard that has been widely adopted across the region, including requirements for merchant authentication and transaction data integrity that provide a baseline level of technical security against the most basic substitution attack vectors.

The commercial digital payment market in Cambodia is populated by a diverse ecosystem of licensed payment service providers, mobile money operators, and bank-affiliated payment applications, operating under licences issued by the NBC under the Law on Negotiable Instruments and Payment Transactions (2005) and the subsequent Payment System Law framework. Major platforms include Wing Money (originally Wing Specialised Bank, now owned by ABA Bank and BRED), TrueMoney Cambodia, Pi Pay, Acleda Bank's digital payment services, and numerous smaller operators. The competition among these platforms for market share has driven rapid innovation in product features and user experience but has also created pressure on security investment and contributed to a fragmented compliance landscape in which regulatory obligations are interpreted and implemented inconsistently across operators.

3.2 Financial Inclusion Achievements and Remaining Gaps

Cambodia's digital payment infrastructure has generated genuine and substantial financial inclusion gains that provide important context for the regulatory analysis that follows. The World Bank's 2021 Global Findex survey found that account ownership among Cambodian adults had increased from 22 percent in 2014 to 33 percent in 2021, with mobile money accounts accounting for a significant share of the increase. Bakong's user base growth — from initial launch to over ten million registered users within four years — substantially exceeds account ownership figures as traditionally measured, reflecting the system's design to enable access through mobile phones without requiring a formal bank account. The

NBC's data suggest that Bakong has achieved particular penetration in rural and peri-urban areas where conventional bank branches are absent, and among lower-income population segments who previously relied entirely on cash or informal money transfer services.

The economic benefits of digital payment adoption for financial inclusion in Cambodia are multiple and well-documented: reduced transaction costs for remittances (both domestic and cross-border), improved access to savings and credit products linked to digital payment accounts, reduced cash handling risks for merchants and consumers, and enhanced capability for government social transfer payments to reach recipients rapidly and with reduced leakage. The NBC's ambition to reduce Cambodia's historically high US dollar usage — estimated at approximately 85 percent of transactions by value at Bakong's launch — has been partially advanced by Bakong's functionality, though the structural factors driving dollarisation (including distrust of the riel and the cross-border commercial relationships that preference US dollar settlement) remain substantially intact.

Significant financial inclusion gaps persist, however, particularly along gender, geographic, and generational dimensions. Rural women — who constitute the majority of Cambodia's agricultural workforce and are disproportionately engaged in informal economic activity — remain substantially underrepresented in digital payment adoption data, reflecting barriers including limited smartphone ownership, lower digital literacy, and the social and cultural norms that in some communities limit women's autonomous engagement with financial services. The elderly population shows markedly lower digital payment adoption, creating a consumer protection challenge as payment infrastructure transitions away from cash-based models that this population understands and trusts.

3.3 Cambodia's Regulatory Architecture for Digital Payments

The NBC's regulatory framework for digital payments is built upon a foundation of legislation that predates the current phase of FinTech development and that has been substantially supplemented through subsidiary regulation, regulatory circulars, and licensing conditions in ways that create a degree of regulatory uncertainty for payment service providers attempting to navigate their obligations. The Law on Negotiable Instruments and Payment Transactions of 2005 provides the primary legislative basis for payment system regulation, authorising the NBC to regulate and supervise payment systems and payment service providers. The NBC has exercised this authority to issue a series of Prakas (regulatory instruments) governing licensing, capital requirements, operational standards, and, increasingly, cybersecurity and consumer protection requirements for payment service providers.

The NBC's Prakas on Payment Service Providers (2016, as amended) establishes licensing categories for payment system operators, payment service providers, and payment instrument issuers, with different capital, operational, and supervisory requirements applying to each category. Cybersecurity requirements for licensed payment service providers are addressed in NBC cybersecurity guidance and are incorporated into licensing conditions, though the specificity and contemporaneity of these requirements has been the subject of criticism from payment security practitioners. The NBC has progressively updated its cybersecurity expectations — incorporating references to international standards including PCI DSS (Payment Card Industry Data Security Standard) and ISO 27001 — but the enforcement of these requirements against licensed payment service providers has been constrained by the NBC's limited supervisory capacity in the cybersecurity domain.

Consumer protection in the digital payment context is addressed through a combination of NBC Prakas provisions governing dispute resolution, transaction reversal, and liability for unauthorised transactions, and through Cambodia's Law on Consumer Protection (2019) administered by the Ministry of Commerce. The allocation of these regulatory responsibilities across two ministries with different mandates and limited coordination mechanisms creates gaps in consumer protection coverage that payment fraud victims have found difficult to navigate. The absence of a dedicated financial consumer protection authority with the mandate, expertise, and enforcement powers to address digital payment consumer complaints has been identified by international observers — including the World Bank's financial sector diagnostic assessments — as a significant structural weakness in Cambodia's financial consumer protection architecture.

4. INTERNATIONAL AND COMPARATIVE REGULATORY FRAMEWORKS FOR DIGITAL PAYMENT SECURITY

4.1 European Union: PSD2, DORA, and Strong Customer Authentication

The European Union's regulatory framework for digital payment security is among the most comprehensive and technically specific in the world, centred on the revised Payment Services Directive (PSD2) and its implementing technical standards, and supplemented by the Digital Operational Resilience Act (DORA) applicable to financial entities including payment institutions. PSD2's requirements for Strong Customer Authentication (SCA) — mandating multi-factor authentication for electronic payment initiation, using at least two of the three factors of knowledge, possession, and inherence — represent the most significant consumer-facing payment security requirement in the EU framework, with substantial demonstrated effectiveness in reducing card-not-present fraud in markets where implementation has been most complete.

PSD2's open banking framework — requiring banks to provide API access to account information and payment initiation services for licensed third-party providers — has generated significant FinTech innovation but has also created new attack surfaces that the

European Banking Authority's technical standards on API security and incident reporting seek to address. The requirement for Third Party Providers (TPPs) to be licensed and to comply with SCA requirements when initiating payments provides a regulatory wrapper around open banking that Cambodia's equivalent regulatory framework does not yet contemplate. PSD2's liability framework — which places liability for unauthorised payment transactions on the payment service provider unless the payer has acted fraudulently or with gross negligence — creates strong incentives for payment providers to invest in security and to resolve consumer disputes promptly, a liability allocation that stands in significant contrast to the less protective frameworks applicable in Cambodia and much of Southeast Asia.

DORA, entering into application in January 2025, extends and deepens the operational resilience requirements for EU financial entities including payment institutions, imposing ICT risk management frameworks, incident classification and reporting obligations, digital operational resilience testing requirements, and third-party ICT risk management obligations that address the supply chain vulnerabilities that have been the source of several major payment system security incidents. DORA's framework for ICT third-party risk management — requiring financial entities to maintain registers of their ICT third-party arrangements, to conduct risk assessments of critical third-party providers, and to ensure contractual provisions that protect against third-party-induced operational disruptions — provides a model for the management of the third-party risks that are particularly acute in Cambodia's payment ecosystem, where multiple payment service providers rely on shared technical infrastructure and common vendors.

4.2 Singapore: MAS Technology Risk Guidelines and Payment Services Act

Singapore's Monetary Authority of Singapore (MAS) has established itself as a global leader in digital payment regulation, combining technologically sophisticated supervisory expectations with a broadly enabling approach to FinTech innovation that has made Singapore the regional hub for digital financial services in Southeast Asia. The MAS Technology Risk Management Guidelines (TRMG), substantially updated in 2021, provide granular technical guidance on cybersecurity and operational resilience requirements for financial institutions including payment service providers, addressing areas including system security, data centre management, software development lifecycle security, cryptographic controls, network security, and cyber threat intelligence.

The Payment Services Act (PSA) 2019, as amended in 2021 to expand its scope, establishes a single licensing framework for a range of digital payment services including account issuance, domestic and cross-border money transfer, e-money issuance, and digital payment token services. The PSA's licensing framework is risk-scaled — operators of larger and higher-risk payment services are subject to more demanding capital, safeguarding, and operational requirements — and its scope explicitly encompasses digital payment token (cryptocurrency) services, addressing a regulatory gap that exists in Cambodia's framework. MAS's consumer protection provisions under the PSA, including requirements for timely dispute resolution, transparent fee disclosure, and safeguarding of customer funds, provide a benchmark for consumer protection standards in the digital payment context that Cambodia's regulatory framework does not yet approximate.

Singapore's Anti-Scam Centre, established in 2019 as a collaboration between the Singapore Police Force and the major banks, provides an operational model for the coordinated detection, reporting, and rapid response to digital payment fraud that has achieved measurable reductions in scam-related losses through faster account freezing and interbank cooperation. Singapore's legislative authorisation for banks to proactively restrict accounts suspected of involvement in scam activity — without waiting for a formal police report or court order — represents a regulatory innovation that enables real-time fraud disruption at a pace that conventional law enforcement mechanisms cannot match. The applicability of this model to Cambodia's more constrained institutional environment would require significant adaptation, but the underlying principle — that payment service providers should have both the authority and the obligation to act proactively to prevent fraud — is directly relevant to Cambodia's consumer protection framework design.

4.3 ASEAN Regional Coordination and the Nexus Bank Initiative

The ASEAN region's approach to digital payment system regulation is characterised by significant diversity across member states — reflecting the wide range of economic development levels, institutional capacities, and regulatory philosophies represented in the bloc — alongside growing efforts at regional coordination driven partly by the practical needs of cross-border payment interoperability. The ASEAN Framework on Digital Data Governance and the ASEAN Digital Integration Framework provide high-level principles for digital financial infrastructure governance, but substantive regulatory harmonisation in the payment domain remains limited. The ASEAN Working Committee on Financial Integration's work on payment systems interconnection has produced the ASEAN Payment Connectivity initiative, which links national fast payment systems across member states, but does not yet encompass harmonised consumer protection or cybersecurity standards for cross-border payment transactions.

The bilateral cross-border QR payment linkages that Cambodia has established with Thailand, Vietnam, and Malaysia under NBC and regional central bank coordination represent an important advance in regional payment interoperability, enabling cross-border QR payments using KHQR-compatible terminals. These linkages, while beneficial for consumers and merchants engaged in cross-border commerce, extend the fraud exposure of Cambodian payment consumers to the security standards of partner country payment systems — and vice versa. The absence of harmonised minimum security standards and consumer protection obligations applicable to cross-border payment transactions conducted through these linkages means that fraud liability and consumer recourse mechanisms may vary significantly depending on which country's payment infrastructure is used for a given transaction, creating gaps that sophisticated fraudsters can exploit.

Thailand's PromptPay system, with which Cambodia's Bakong has established a cross-border linkage, provides a useful comparative reference for the consumer protection architecture that Cambodia's system should aspire to. PromptPay's consumer protection framework — established under the Bank of Thailand's Payment Systems Act and the Electronic Transactions Act — includes clear liability rules for unauthorised transactions, mandatory fraud reporting and response obligations for payment service providers, and the Bank of Thailand's active consumer complaints handling function that provides accessible recourse for consumers who have suffered payment fraud losses. The integration of these consumer protection standards into the bilateral Bakong-PromptPay linkage framework would represent a significant improvement in the protection available to Cambodian consumers using cross-border payment services.

5. CAMBODIA'S DIGITAL PAYMENT INFRASTRUCTURE AND CYBER-ENABLED FINANCIAL CRIME

5.1 The Exploitation of Digital Payment Channels for Money Laundering

The relationship between Cambodia's digital payment infrastructure and the country's endemic cyber-enabled financial crime ecosystem is one of deep and troubling interdependency. The billions of dollars generated annually by scam compound operations across Cambodia's border zones and coastal enclaves require laundering — conversion from the proceeds of crime into apparently legitimate financial assets — through channels capable of handling large transaction volumes rapidly and with opacity sufficient to frustrate financial intelligence analysis. Cambodia's digital payment ecosystem, with its multiple licensed and unlicensed operators, its integration of USDT and other cryptocurrency functionality, and its regulatory oversight gaps, provides precisely such channels.

The money laundering methodologies employed in Cambodia's digital payment infrastructure span the spectrum from relatively simple to highly sophisticated. At the simpler end, fraud victims are directed to send payments to accounts held within Cambodian-licensed payment service providers that serve as the initial collection point for stolen funds, with the funds subsequently withdrawn in cash, transferred to cryptocurrency wallets, or moved through chains of domestic transfers before extraction. More sophisticated layering involves the use of multiple tiers of payment accounts — some held with licensed providers, others in informal value transfer networks — combined with cryptocurrency conversion and cross-border transfers that exploit the interoperability linkages between Bakong and partner country payment systems to move value across borders before anti-money laundering alerts can be triggered.

The role of USDT in Cambodia's financial crime ecosystem deserves specific analysis. Tether's USDT is the stablecoin of choice for scam compound money laundering across Southeast Asia, selected for its combination of dollar-denominated value stability (which preserves the purchasing power of stolen funds during the laundering process), global exchangeability (enabling value transfer across jurisdictions without the friction of currency conversion), and availability through exchanges and over-the-counter brokers in Cambodia and neighbouring countries that apply inadequate know-your-customer and anti-money laundering controls. The NBC's decision to integrate USDT functionality into the Bakong platform — enabling USDT transfers through the same infrastructure used for riel and US dollar payments — has been criticised by anti-money laundering experts who argue that it extends the regulatory legitimacy of the NBC's infrastructure to a payment instrument whose specific use in Cambodia is dominated by criminal activity.

5.2 FATF Mutual Evaluation and Cambodia's AML/CFT Deficiencies

The Financial Action Task Force (FATF) and its Asia/Pacific Group on Money Laundering (APG) have assessed Cambodia's anti-money laundering and counter-terrorist financing (AML/CFT) framework through multiple mutual evaluation cycles, consistently identifying significant deficiencies in both the legal framework and its effective implementation. Cambodia was placed on the FATF 'grey list' (Jurisdictions under Increased Monitoring) in February 2019, a designation that reflects identified strategic deficiencies in the country's AML/CFT regime and imposes enhanced scrutiny on Cambodia's financial transactions by correspondent banks and international financial institutions. Although Cambodia was removed from the grey list in October 2023 following the implementation of a series of FATF Action Plan items, the APG's assessment of Cambodia's compliance with FATF Recommendations remains mixed, with significant deficiencies noted in the effectiveness of supervision of designated non-financial businesses and professions, the investigation and prosecution of money laundering cases, and the implementation of beneficial ownership transparency requirements.

The specific application of FATF's Recommendations to digital payment service providers in Cambodia has been inadequate in several documented respects. Customer due diligence requirements — requiring payment service providers to identify and verify the identity of their customers, to understand the nature and purpose of customer relationships, and to conduct ongoing monitoring of transactions — have been inconsistently implemented across the sector, with smaller and less well-resourced operators demonstrating significant compliance gaps. The FATF Recommendation 16 'travel rule' — requiring the transmission of originator and beneficiary information with cross-border wire transfers and, under updated FATF guidance, with virtual asset transfers — has not been comprehensively implemented for Cambodia's cross-border payment and cryptocurrency transactions, creating an information gap that prevents effective tracing of suspicious transaction flows across jurisdictions.

The NBC's Financial Intelligence Unit (FIU), established under the Law on Anti-Money Laundering and Combating the Financing of Terrorism (2007, as amended in 2020), receives suspicious transaction reports from financial institutions and designated non-financial businesses and is responsible for analysing these reports and disseminating financial intelligence to law enforcement. The volume and quality of suspicious transaction reporting from digital payment service providers has been identified as a significant weakness in Cambodia's financial intelligence system — reflecting both the compliance capability gaps of payment service providers and the chilling effect on reporting of an institutional environment in which the relationship between financial intelligence and law enforcement consequences for reported entities is not clearly understood or trusted by reporting entities.

5.3 Consumer Fraud in Cambodia's Digital Payment Market

Beyond the systemic money laundering challenge, Cambodia's digital payment consumers face a diverse and escalating range of direct fraud threats that the current regulatory framework is poorly equipped to prevent or remediate. Impersonation fraud — in which fraudsters contact consumers by phone or messaging application, impersonating NBC officials, commercial bank staff, tax authority representatives, or law enforcement officers, and persuade victims to make urgent payments or to disclose account credentials — has become the dominant consumer payment fraud typology in Cambodia, exploiting the relatively low digital financial literacy of a population that has adopted digital payment systems rapidly without commensurate security education.

Investment fraud through digital payment channels — the same pig butchering model that drives Cambodia's scam compound operations when directed at overseas victims — is also inflicted on domestic Cambodian consumers, who are targeted through social media platforms and messaging applications with fraudulent investment opportunities in cryptocurrency, foreign exchange trading, and online gaming platforms that accept payment through digital wallets. Cambodian consumers who fall victim to these schemes typically have no effective recourse: the relevant payment service provider may contend that the consumer authorised the transaction; the NBC's consumer complaint mechanisms are not designed to address fraud losses; and the criminal justice system's capacity to investigate and prosecute digital payment fraud is severely constrained by resource, skill, and institutional capacity limitations.

6. STRUCTURAL LEGAL DEFICIENCIES IN CAMBODIA'S DIGITAL PAYMENT CONSUMER PROTECTION FRAMEWORK

6.1 The Absence of Liability Rules for Unauthorised Transactions

Perhaps the most consequential structural deficiency in Cambodia's digital payment consumer protection framework is the absence of clear, enforceable, and consumer-protective liability rules governing unauthorised payment transactions. In the European Union, PSD2 Article 73 places liability for unauthorised payment transactions squarely on the payment service provider unless it can demonstrate that the payer acted fraudulently or with gross negligence — a liability allocation that creates strong provider incentives for security investment and rapid fraud response. In Singapore, MAS guidelines on consumer liability for unauthorised transactions similarly protect consumers against losses from unauthorised transactions where the consumer has not been negligent or complicit.

Cambodia's regulatory framework does not establish equivalent consumer-protective liability rules. The NBC's Prakas provisions on consumer dispute resolution for payment transactions address the process for submitting complaints but do not clearly specify the liability of payment service providers for losses arising from unauthorised transactions effected as a result of security failures in the provider's systems. In practice, Cambodian consumers who suffer losses from payment fraud — whether through unauthorised access to their accounts, QR code substitution attacks, or social engineering that results in fraudulent transactions — are frequently told by their payment service provider that the transaction was 'authorised' (in the sense that the correct credentials were used or a QR code was scanned) and that the provider bears no liability for the resulting loss. This outcome, which would be legally untenable in jurisdictions with PSD2-equivalent consumer protection rules, is the standard experience of Cambodian payment fraud victims.

The reform of liability rules for unauthorised payment transactions is arguably the single most impactful consumer protection improvement that Cambodia's regulatory framework could achieve in the digital payment context. Clear rules placing presumptive liability on payment service providers for losses arising from unauthorised transactions, with defined exceptions for payer negligence or fraud, would align incentives between providers and consumers in a manner that drives security investment, rapid fraud response, and genuine commitment to customer protection that current regulatory arrangements do not produce.

6.2 Data Protection and Cybersecurity Legal Gaps

Cambodia's data protection legal framework is nascent and inadequate to the requirements of a modern digital payment ecosystem. The country lacks a comprehensive personal data protection law, despite years of drafting and consultation processes that have not yet produced enacted legislation as of mid-2025. In the absence of a general data protection framework, the protection of the personal and financial data generated by digital payment transactions relies on sector-specific regulatory provisions, the terms and conditions of payment service provider customer agreements (which are negotiated from a position of fundamental consumer disadvantage), and the general provisions of Cambodia's Law on E-Commerce (2019) that address electronic data security in general terms. The protection these provisions offer is substantially inferior to the GDPR-equivalent frameworks that apply in Singapore, Thailand (Personal Data Protection Act 2019), Vietnam (Personal Data Protection Decree 2023), and an increasing number of ASEAN member states.

The cybercrime legal framework is similarly limited. Cambodia's Law on Telecommunications (2015) and its implementing regulations contain provisions addressing unauthorised access to computer systems and electronic communications, but these provisions are narrowly framed and have rarely been invoked in the context of digital payment fraud. The absence of a comprehensive cybercrime law specifically addressing digital payment fraud, phishing, SIM swapping, account takeover, and related offences creates substantive criminal law gaps that prosecutors cannot bridge through creative interpretation of the telecommunications legislation. The result is that the perpetrators of digital payment fraud against Cambodian consumers — where they are domestic actors susceptible to Cambodian jurisdiction — face minimal criminal law consequences for their conduct.

The NBC's cybersecurity requirements for licensed payment service providers, while progressively strengthened, remain below the standards that the complexity and value of Cambodia's digital payment ecosystem warrants. The absence of mandatory penetration testing requirements, security incident notification obligations to the NBC and to affected consumers, and minimum technical security standards aligned with current international benchmarks means that the NBC's supervisory oversight of payment service provider cybersecurity is based on self-reported compliance rather than independently verified security assurance. The implementation of mandatory third-party security audits and penetration testing for payment service providers above defined transaction volume thresholds, aligned with PCI DSS requirements and supervised by the NBC, would substantially improve the quality of security oversight in the sector.

6.3 Enforcement Capacity and Institutional Coordination Gaps

The effectiveness of any legal framework for digital payment consumer protection is ultimately dependent on the capacity of regulatory authorities to enforce its provisions — to detect violations, to investigate complaints, to impose meaningful consequences for non-compliance, and to coordinate across the multiple agencies whose mandates intersect in the digital payment domain. Cambodia's regulatory framework suffers from significant enforcement capacity gaps across all of these dimensions. The NBC's supervisory staff dedicated to payment system oversight and financial consumer protection are few in number relative to the complexity and growth of the sector they supervise. The Ministry of

Commerce's consumer protection function has limited expertise in digital financial services and limited coordination with the NBC on payment-specific consumer issues. The Cambodia Financial Intelligence Unit's analytical capacity is constrained by staffing and technology limitations that limit its ability to identify the complex layering techniques through which payment fraud proceeds are laundered.

The judicial capacity to adjudicate digital payment consumer disputes is similarly limited. Courts lack specialised expertise in digital payment technology, and the cost and complexity of civil litigation in Cambodia makes the courts an inaccessible dispute resolution mechanism for the individual consumer fraud victims who typically suffer losses in amounts that do not justify the transaction costs of litigation. The development of accessible, low-cost alternative dispute resolution mechanisms specifically for digital payment consumer complaints — as exist in Singapore (Financial Industry Disputes Resolution Centre), Thailand (OMBUDSMAN Financial), and numerous other jurisdictions — represents an important institutional reform that Cambodia's framework does not yet encompass.

7. A NORMATIVE REFORM AGENDA FOR CAMBODIA'S DIGITAL PAYMENT LEGAL FRAMEWORK

7.1 Enacting a Personal Data Protection Law

The enactment of a comprehensive personal data protection law is the foundational legal reform required to underpin consumer protection in Cambodia's digital payment ecosystem. A data protection law aligned with international standards — including the ASEAN Model Contractual Clauses for Cross Border Data Flows, the APEC Privacy Framework, and the substantive principles of the GDPR — would establish enforceable rights for consumers regarding the collection, processing, and security of their personal and financial data by payment service providers, impose mandatory data breach notification obligations, and establish an independent data protection authority with investigative and enforcement powers. The law should incorporate specific provisions addressing the heightened sensitivity of financial data, including payment transaction history, biometric authentication data, and the account and device identifiers that constitute the identity infrastructure of digital payment systems.

The personal data protection law should be designed with explicit attention to the cross-border data flows that characterise Cambodia's digital payment ecosystem, establishing clear rules for the transfer of Cambodian consumer payment data to the foreign-based technical infrastructure providers and payment network operators upon whom Cambodia's payment service providers rely. The absence of such rules creates a legal vacuum in which

Cambodian consumer payment data may be transferred to and processed in jurisdictions with substantially lower data protection standards, with no legal basis for requiring those third parties to protect the data in accordance with the standards applicable in Cambodia.

7.2 Reform of Payment Service Provider Liability Rules

The NBC should issue a Prakas establishing clear, consumer-protective liability rules for unauthorised payment transactions conducted through licensed payment service providers, aligned with the PSD2 model of presumptive provider liability subject to defined exceptions. The liability framework should establish that: payment service providers bear presumptive liability for losses arising from unauthorised transactions; the burden of proof for establishing the consumer's negligence or fraud lies with the provider; maximum consumer liability for losses from specific categories of fraud (including account takeover and impersonation fraud) is capped at defined amounts; and providers are required to refund disputed transaction amounts provisionally pending investigation, rather than requiring consumers to wait for investigation completion before receiving any remediation.

The liability reform should be accompanied by mandatory fraud loss reporting requirements for payment service providers, requiring periodic disclosure to the NBC of fraud loss data segmented by fraud typology, transaction channel, and consumer demographic — data that the NBC currently does not systematically collect but that is essential for evidence-based regulatory policy development. The publication of fraud loss data at the sector level (while protecting commercially sensitive provider-specific data) would enable consumers to make informed comparisons of payment providers' fraud protection track records and would create market incentives for security investment that complement regulatory obligations.

7.3 Strengthening AML/CFT for Digital Payment Channels

The NBC should implement, through Prakas and supervisory guidance, a comprehensive and contemporarily calibrated AML/CFT framework specifically addressing digital payment channels, including customer due diligence requirements proportionate to the risk profile of different payment channels and transaction types, the travel rule for digital payment transactions and cryptocurrency transfers, transaction monitoring parameters calibrated to the fraud and money laundering patterns prevalent in Cambodia's digital payment market, and mandatory suspicious transaction reporting obligations specifically addressing digital payment fraud and cryptocurrency layering patterns. Supervisory examination of payment service providers' AML/CFT programmes should be conducted on a regular and risk-based schedule, with examination findings informing both individual remediation requirements and sector-wide supervisory guidance.

The NBC's FIU should develop specific financial intelligence products addressing digital payment fraud and cryptocurrency money laundering patterns in Cambodia, disseminated to payment service providers as supervisory guidance and shared with law enforcement and international FIU partners through the Egmont Group and bilateral financial intelligence cooperation channels. The establishment of a dedicated anti-scam unit within the NBC or Cambodia National Police — modelled on Singapore's Anti-Scam Centre — with authority to issue rapid account freeze directions to payment service providers on the basis of scam intelligence, would provide the operational capability for real-time fraud disruption that Cambodia's current institutional arrangements do not support.

7.4 USDT and Cryptocurrency Regulatory Framework

The regulatory framework for cryptocurrency and stablecoin transactions in Cambodia requires urgent development, given the pervasive use of USDT and other digital assets in the country's money laundering ecosystem. The NBC should establish a clear licensing or registration regime for virtual asset service providers (VASPs) operating in Cambodia, aligned with FATF's Recommendation 15 on virtual assets and its 2021 updated guidance on virtual assets and VASPs. The regime should impose AML/CFT obligations on VASPs including customer due diligence, transaction monitoring, suspicious transaction reporting, and travel rule compliance for cryptocurrency transfers, and should require VASPs to implement technical controls enabling the tracing of transaction chains for law enforcement purposes.

The NBC's decision to integrate USDT functionality into the Bakong platform should be reconsidered in light of the demonstrated use of this functionality for money laundering, or at minimum conditioned on the implementation of technical and procedural controls capable of meaningfully reducing the platform's exposure to money laundering abuse. Technical measures that the NBC should require for USDT transactions processed through Bakong include transaction velocity and amount limits calibrated to legitimate remittance use cases, mandatory blockchain analytics screening of USDT transaction counterparties against known criminal addresses, and real-time suspicious transaction reporting triggers linked to the NBC's FIU monitoring systems.

7.5 Regional Cooperation and ASEAN Integration

Cambodia's digital payment consumer protection challenges are not resolvable through domestic regulatory reform alone — the cross-border character of both legitimate digital payment flows and the criminal exploitation of Cambodia's payment infrastructure makes regional and international regulatory cooperation essential. Cambodia should actively engage in the development of ASEAN-level minimum standards for digital payment consumer protection, AML/CFT obligations for payment service providers, and cybersecurity requirements for cross-border payment linkages, through the ASEAN Working Committee on Financial Integration and the ASEAN Experts Group on Competition. The bilateral payment linkages that Cambodia has established with Thailand, Vietnam, and Malaysia should be upgraded to incorporate harmonised consumer protection obligations applicable to cross-border transactions, including clear liability rules and accessible consumer complaint mechanisms for consumers in both countries.

Capacity building cooperation — through which Cambodia can access the expertise and institutional experience of more advanced regional regulatory frameworks — should be pursued through structured partnerships with the Bank of Thailand, MAS Singapore, and Bank Indonesia, all of whom have offered technical assistance to NBC on payment system regulation in recent years. The World Bank, Asian Development Bank, and International Monetary Fund have active technical assistance programmes in Cambodia's financial sector, and these programmes should be directed to include a specific focus on digital payment consumer protection law reform and financial intelligence capability development, alongside the macroeconomic and prudential regulatory priorities that have historically dominated the international financial institution engagement with Cambodia's financial sector.

8. CONCLUSION

Cambodia's digital payment story is a story of two realities coexisting within the same regulatory space, served by the same infrastructure, and nominally governed by the same legal framework. One reality is the Bakong-enabled financial inclusion of millions of rural Cambodians who can now receive remittances, pay utility bills, and access basic financial services from their mobile phones — a genuine development achievement that represents the transformative potential of digital financial infrastructure. The other reality is the same Bakong infrastructure being used as a laundering channel for the billions of dollars generated by the scam compound operations that have made Cambodia internationally notorious for cyber-enabled financial crime — a reality that represents one of the most acute governance failures in the contemporary digital financial landscape.

The legal framework that governs these two realities is inadequate to the demands of either. For the financially included Cambodian consumer seeking protection against payment fraud, the framework offers ambiguous liability rules, inaccessible dispute resolution, and a regulatory architecture whose enforcement capacity falls far short of the supervisory demands of a sector growing at Cambodia's pace. For the international community seeking to disrupt the criminal exploitation of Cambodia's payment infrastructure, the framework offers limited AML/CFT tools, weak cryptocurrency regulation, insufficient financial intelligence capacity, and governance integrity deficits that undermine the effectiveness of those tools that exist.

The reform agenda advanced in this article — data protection legislation, payment service provider liability reform, comprehensive AML/CFT for digital channels, cryptocurrency regulatory framework, and regional cooperation — is ambitious relative to Cambodia's current institutional capacity and political economy. But the cost of inaction is measured not only in the fraud losses suffered by Cambodian consumers and the reputational damage that criminal exploitation of the country's payment infrastructure inflicts on its international economic relationships, but in the damage to the long-term sustainability of the digital payment ecosystem itself. Consumer trust is the foundation upon which digital financial inclusion rests; if that trust is eroded by fraud losses and the perception of regulatory indifference, the financial inclusion gains of the past decade will prove fragile. The law's role is to build and sustain that trust by ensuring that the digital payment systems Cambodian consumers depend upon are governed in a manner commensurate with the value — and the risks — they represent.

REFERENCES

Allen, F. et al., 'The Foundations of Financial Inclusion: Understanding Ownership and Use of Formal Accounts' (2016) 13(1) Journal of Financial Intermediation 1.

ASEAN Secretariat, 'ASEAN Framework on Digital Data Governance' (ASEAN, 2021).

Asia/Pacific Group on Money Laundering (APG), 'Mutual Evaluation Report: Kingdom of Cambodia' (APG, 2017).

Asia/Pacific Group on Money Laundering (APG), 'Follow-Up Report: Cambodia' (APG, 2023).

Bank for International Settlements (BIS), 'Central Bank Digital Currencies for Cross-Border Payments' (BIS, 2021).

Bank of Thailand, 'Payment Systems Act B.E. 2560 (2017)' (Bank of Thailand, 2017).

Cambodia, Law on Anti-Money Laundering and Combating the Financing of Terrorism (2007, amended 2020).

Cambodia, Law on Consumer Protection (2019).

Cambodia, Law on E-Commerce (2019).

Cambodia, Law on Negotiable Instruments and Payment Transactions (2005).

Cambodia, Law on Telecommunications (2015).

Digital Operational Resilience Act (DORA), Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022.

European Banking Authority (EBA), 'Report on the Implementation of the EBA Guidelines on Major Incident Reporting under PSD2' (EBA, 2022).

Financial Action Task Force (FATF), 'Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (FATF, 2021).

Financial Action Task Force (FATF), 'High-Risk and Other Monitored Jurisdictions' (FATF, October 2023).

Goldsmith-Pinkham, P., Sokolinski, S. and Vainstein, Y., 'The Consumer Welfare Impact of FinTech Borrowing' (2023) National Bureau of Economic Research Working Paper No. 31596.

Hayashi, F. and Markiewicz, E., 'Payment System Improvement — Public Consultation Paper' (Federal Reserve Bank of Kansas City, 2013).

International Monetary Fund (IMF), 'Cambodia: Financial Sector Assessment Program' (IMF Country Report No. 22/291, 2022).

Klapper, L., El-Zoghbi, M. and Hess, J., 'Achieving the Sustainable Development Goals: The Role of Financial Inclusion' (CGAP, 2016).

Monetary Authority of Singapore (MAS), 'Technology Risk Management Guidelines' (MAS, 2021).

Monetary Authority of Singapore (MAS), 'Payment Services Act 2019' (MAS, 2019, as amended 2021).

National Bank of Cambodia (NBC), 'Annual Report 2023' (NBC, 2024).

National Bank of Cambodia (NBC), 'Bakong: Cambodia's Retail Payment System' (NBC, 2022).

National Bank of Cambodia (NBC), 'Prakas on Payment Service Providers' (NBC, 2016, as amended).

Revised Payment Services Directive (PSD2), Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015.

Soramitsu, 'Bakong: The World's First Production Blockchain-Based Retail CBDC' (Soramitsu Technical Report, 2021).

Thailand, Personal Data Protection Act B.E. 2562 (2019).

United Nations Office on Drugs and Crime (UNODC), 'Casinos, Cyber Fraud and Trafficking in Persons for Forced Criminality in Southeast Asia' (UNODC, 2023).

World Bank, 'Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19' (World Bank, 2022).

World Bank, 'Cambodia Financial Sector Development Strategy 2021–2025' (World Bank / Royal Government of Cambodia, 2021).

Zerzan, A., 'New Technologies, New Risks? Innovation and Countering the Financing of Terrorism' (World Bank Working Paper No. 178, 2009).